Amendments to the Claims:

Listing of the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) An encrypting apparatus comprising:

an encrypting operation section carrying out an encrypting operation to a plaintext using intermediate data at each of a plurality of encrypting stages of said encrypting operation to produce a ciphertext, wherein said encrypting operation section outputs encrypting stage data indicating an encrypting state at each of said plurality of processing stages;

a determining section determining whether said encrypting operation at a next encrypting stage should be changed, based on said encrypting stage data at a current encrypting stage from said encrypting operation section; and

a control section changing said encrypting operation at said next encrypting stage a plurality of times when it is determined that said encrypting operation at said next encrypting stage should be changed,

wherein said determining section determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting stage data at said current encrypting stage from said encrypting operation section,

wherein said encrypting stage data includes said intermediate data at said next encrypting stage, and

wherein said control section changes said intermediate data at said next encrypting stage a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation,

wherein said encrypting operation section divides each n-bit word of the plaintext into an upper n bits and a lower n bits, n being an even integer value greater than or equal to 16,

wherein said determining section calculates a logical product of the upper n bits of the plaintext with at least one of said plurality of random numbers to obtain a first result, and said determining section calculates a logical product of the lower n bits of the plaintext with at least one of said plurality of random numbers to obtain a second result,

wherein, in obtaining the first result and the second result, a first subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a first of said plurality of random numbers, a second subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a second of said plurality of random numbers, and a third subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with both the first and second random numbers.

2. (Previously Presented) An encrypting apparatus according to claim 1, wherein said determining section determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed based on whether or not said current encrypting stage from said encrypting operation section is determined to be a stage to determine a random number conditional branch.

3. (Previously Presented) An encrypting apparatus according to claim 2, wherein said control section changes said intermediate data at said next encrypting stage depending on said plaintext or a data dependent on said plaintext in place of said random numbers.

4. (Previously Presented) An encrypting apparatus according to claim 1, wherein said determining section determines whether an encrypting procedure at said next encrypting stage of said encrypting operation should be changed depending on at least a random number, based on said encrypting stage data at said current encrypting stage from said encrypting operation section, and

wherein said control section changes said encrypting procedure at said next encrypting stage of said encrypting operation depending on said random numbers.

5. (Previously Presented) An encrypting apparatus according to claim 4, wherein said control section changes said encrypting procedure at said next encrypting stage of said encrypting operation depending on said plaintext or a data dependent on said plaintext in place of said random numbers.

6. (Previously Presented) An encrypting apparatus according to claim 1, wherein said determining section determines whether said encrypting operation at said next

encrypting stage should be changed depending on at least a random number, based on said encrypting stage data at said current encrypting stage from said encrypting operation section, and

wherein said control section inserts a delay time in said encrypting operation at said next encrypting stage depending on said random numbers.

7. (Previously Presented) An encrypting apparatus according to claim 6, wherein said control section inserts said delay time in said encrypting operation at said next encrypting stage depending on said plaintext or a data dependent on said plaintext in place of said random numbers.

8. (Currently Amended) A decrypting apparatus comprising:

a decrypting operation section carrying out a decrypting operation to a ciphertext using intermediate data at each of a plurality of decrypting stages of said decrypting operation to produce a plaintext. wherein said decrypting operation section outputs decrypting stage data indicating a decrypting state at each of said plurality of decrypting stages;

a determining section determining whether said decrypting operation at a next decrypting stage should be changed, based on said decrypting stage data at a current decrypting stage from said decrypting operation section; and

a control section changing said decrypting operation at said next decrypting stage a plurality of times when it is determined that said decrypting operation at said next decrypting stage should be changed,

wherein said determining section determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed depending on at least a plurality of random numbers, based on said decrypting stage data at said current decrypting stage from said decrypting operation section,

wherein said decrypting stage data includes said intermediate data for said next decrypting stage, and

wherein said control section changes said intermediate data at said next decrypting stage a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said decrypting operation.

wherein said decrypting operation section divides each n-bit word of the plaintext into an upper n bits and a lower n bits, n being an even integer value greater than or equal to 16,

wherein said determining section calculates a logical product of the upper n bits of the plaintext with at least one of said plurality of random numbers to obtain a first result, and said determining section calculates a logical product of the lower n bits of the plaintext with at least one of said plurality of random numbers to obtain a second result,

wherein, in obtaining the first result and the second result, a first subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a first of said plurality of random numbers, a second subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a second of said plurality of random numbers, and a third subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with both the first and second random numbers.

9. (Previously Presented) A decrypting apparatus according to claim 8, wherein said determining section determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed based on whether or not said current decrypting stage from said decrypting operation section is determined to be a stage to determine a random number conditional branch.

10. (Previously Presented) A decrypting apparatus according to claim 9, wherein said control section changes said intermediate data at said next decrypting stage depending on said ciphertext or a data dependent on said ciphertext in place of said random numbers.

11. (Previously Presented) A decrypting apparatus according to claim 8, wherein said determining section determines whether a decrypting procedure at said next decrypting stage of said decrypting operation should be changed depending on at least a random number, based on said stage data at said current decrypting stage from said decrypting operation section, and

wherein said control section changes said decrypting procedure at said next decrypting stage of said decrypting operation depending on said random numbers.

12. (Previously Presented) A decrypting apparatus according to claim 11, wherein said control section changes said decrypting procedure at said next decrypting stage of said decrypting operation depending on said ciphertext or a data dependent on said ciphertext in place of said random numbers.

13. (Previously Presented) A decrypting apparatus according to claim 8, wherein said determining section determines whether said decrypting operation at said next decrypting stage should be changed depending on at least a random number, based on said stage data at said current decrypting stage from said decrypting operation section, and

wherein said control section inserts a delay time in said decrypting operation at said next decrypting stage depending on said random numbers.

14. (Previously Presented) A decrypting apparatus according to claim 13, wherein said control section inserts said delay time in said decrypting operation at said next decrypting stage depending on said ciphertext or a data dependent on said ciphertext in place of said random numbers.

15. (Currently Amended) An encrypting and decrypting apparatus comprising:

an encrypting and decrypting operation section determining whether an inputted instruction is an encrypt instruction or a decrypt instruction, carrying out an encrypting operation to an inputted text in response to said encrypt instruction using first intermediate data at each of a plurality of encrypting stages of said encrypting operation to produce a ciphertext, and carrying out a decrypting operation to said inputted text in response to said decrypt instruction using second intermediate data at each of a plurality of decrypting stages of said decrypting operation to produce a plaintext, wherein said encrypting and decrypting operation section outputs encrypting stage data indicating an encrypting state at each of said plurality of encrypting stages and outputs decrypting stage data indicating a decrypting state at each of said plurality of decrypting stages;

a determining section determining whether said encrypting operation at a next encrypting stage should be changed, based on said encrypting stage data at a current encrypting stage from said encrypting and decrypting operation section, and determining whether said decrypting operation at a next decrypting stage should be changed, based on said

decrypting stage data at a current decrypting stage from said encrypting and decrypting operation section; and

a control section changing said encrypting operation at said next encrypting stage a plurality of times when it is determined that said encrypting operation at said next encrypting stage should be changed, and changing said decrypting operation at said next decrypting stage a plurality of times when it is determined that said decrypting operation at said next decrypting stage should be changed,

wherein said determining section determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting stage data at said current encrypting stage from said encrypting operation section,

wherein said encrypting stage data includes said intermediate data at said next encrypting stage,

wherein said control section changes said intermediate data at said next encrypting stage a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation,

wherein said determining section determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed depending on at least a plurality of random numbers, based on said decrypting stage data at said current decrypting stage from said decrypting operation section,

wherein said decrypting stage data includes said intermediate data for said next decrypting stage, and

wherein said control section changes said intermediate data at said next decrypting stage a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said decrypting operation,

wherein said encrypting and decrypting operation section divides each n-bit word of the plaintext into an upper n bits and a lower n bits, n being an even integer value greater than or equal to 16,

wherein said determining section calculates a logical product of the upper n bits of the plaintext with at least one of said plurality of random numbers to obtain a first result, and said determining section calculates a logical product of the lower n bits of the plaintext with at least one of said plurality of random numbers to obtain a second result,

wherein, in obtaining the first result and the second result, a first subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a first of said plurality of random numbers, a second subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a second of said plurality of random numbers, and a third subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with both the first and second random numbers.

16. (Previously Presented) An encrypting and decrypting apparatus according to claim 15, wherein said determining section determines whether said first intermediate data at said next encrypting stage of said encrypting operation should be changed depending on a first plurality of random numbers, based on whether or not said current encrypting stage from said encrypting and decrypting operation section is determined to be a stage to determine a random number conditional branch, and said determining section determines whether said second intermediate data at said next decrypting stage of said decrypting operation should be changed depending on a second plurality of random numbers, based on whether or not said current decrypting stage from said encrypting and decrypting operation section is determined to be a stage to determine a random number conditional branch.

17. (Previously Presented) An encrypting and decrypting apparatus according to claim 16, wherein said control section changes said first intermediate data at said next encrypting stage depending on said inputted text or a data dependent on said inputted text in place of said first plurality of random numbers, and changes said second intermediate data at said next decrypting stage depending on said inputted text or said data dependent on said inputted text in place of said second plurality of random numbers.

18. (Previously Presented) An encrypting and decrypting apparatus according to claim 15, wherein said determining section determines whether an encrypting procedure at said next encrypting stage of said encrypting operation should be changed depending on a first plurality of random numbers, based on said encrypting stage data at said current encrypting stage from said encrypting and decrypting operation section, and determines whether a decrypting procedure at said next decrypting stage of said decrypting operation should be changed depending on a second plurality of random numbers, based on

said decrypting stage data at said current decrypting stage from said encrypting and decrypting operation section, and

wherein said control section changes said encrypting procedure at said next encrypting stage of said encrypting operation depending on said first plurality of random numbers and changes said decrypting procedure at said next decrypting stage of said decrypting operation depending on said second plurality of random numbers.

19. (Previously Presented) An encrypting and decrypting apparatus according to claim 18, wherein said control section changes said encrypting procedure at said next encrypting stage of said encrypting operation depending on said inputted text or a data dependent on said inputted text in place of said plurality of random numbers, and changes said decrypting procedure at said next decrypting stage of said decrypting operation depending on said inputted text or said data dependent on said inputted text in place of said plurality of random numbers.

20. (Previously Presented) An encrypting and decrypting apparatus according to claim 15, wherein said determining section determines whether said encrypting operation at said next encrypting stage should be changed depending on a first plurality of random numbers, based on said encrypting stage data at said current encrypting stage from said encrypting and decrypting operation section, and determines whether said decrypting operation at said next decrypting stage should be changed depending on a second plurality of random numbers, based on said decrypting stage data at said current decrypting stage from said encrypting and decrypting operation section, and

wherein said control section inserts a first delay time in said encrypting operation at said next encrypting stage depending on said first random number and inserts a second delay time in said decrypting operation at said next decrypting stage depending on said second plurality of random numbers.

21. (Previously Presented) An encrypting and decrypting apparatus according to claim 20, wherein said control section inserts said first delay time in said encrypting operation at said next encrypting stage depending on said inputted text or a data dependent on said inputted text in place of said first plurality of random numbers, and inserts said second delay time in said decrypting operation at said next decrypting stage depending

on said inputted text or said data dependent on said inputted text in place of said second plurality of random numbers.

22. (Currently Amended) An encrypting method comprising:

(a) determining whether an encrypting operation at a current encrypting stage should be changed, based on encrypting stage data at a previous encrypting stage, said encrypting stage data at said previous encrypting stage indicating an encrypting state at said previous encrypting stage;

(b) changing said encrypting operation at said current encrypting stage when it is determined that said encrypting operation at said current encrypting stage should be changed;

(c) carrying out said encrypting operation at said current encrypting stage a plurality of times to a plaintext using intermediate data at said current encrypting stage; and

(d) executing said steps (a) to (c) to each of a plurality of said encrypting stages of said encrypting operation to produce a ciphertext,

wherein said step (b) determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting stage data at said current encrypting stage from said step (c),

wherein said encrypting stage data includes said intermediate data at said next encrypting stage, and

wherein, in said step (c), said intermediate data at said next encrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation,

wherein said encrypting operation is carried out by:

i) dividing each n-bit word of the plaintext into an upper n bits and a lower n bits, n being an even integer value greater than or equal to 16,

ii) calculating a logical product of the upper n bits of the plaintext with at least one of said plurality of random numbers to obtain a first result, and

iii) calculating a logical product of the lower n bits of the plaintext with at least one of said plurality of random numbers to obtain a second result,

wherein, in obtaining the first result and the second result, a first subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a first of said plurality of random numbers, a second subset of the upper n bits and the lower n bits of the plaintext are

exclusive-or'ed with a second of said plurality of random numbers, and a third subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with both the first and second random numbers.

23. (Previously Presented) An encrypting method according to claim 22, wherein said determining includes:

determining whether said intermediate data at said current encrypting stage of said encrypting operation should be changed depending on a plurality of random numbers, based on said encrypting stage data at said previous encrypting stage.

24. (Previously Presented) An encrypting method according to claim 23, wherein said changing includes:

changing said intermediate data at said current encrypting stage depending on said plaintext or a data dependent on said plaintext in place of said plurality of random numbers.

25. (Previously Presented) An encrypting method according to claim 22, wherein said determining includes:

determining whether an encrypting procedure at said current encrypting stage of said encrypting operation should be changed depending on a plurality of random numbers, based on said encrypting stage data at said previous encrypting stage, and

wherein said changing includes:

changing said encrypting procedure at said current encrypting stage of said encrypting operation depending on said plurality of random numbers.

26. (Previously Presented) An encrypting method according to claim 25, wherein said changing includes:

changing said encrypting procedure at said next encrypting stage of said encrypting operation depending on said plaintext or a data dependent on said plaintext in place of said plurality of random numbers.

27. (Previously Presented) An encrypting method according to claim 22, wherein said determining includes:

determining whether said encrypting operation at said current encrypting stage should be changed depending on a plurality of random numbers, based on said encrypting stage data at said previous encrypting stage, and

wherein said changing includes:

inserting a delay time in said encrypting operation at said current encrypting stage depending on said plurality of random numbers.

28. (Previously Presented) An encrypting method according to claim 27, wherein said changing includes:

inserting said delay time in said encrypting operation at said current encrypting stage depending on said plaintext or a data dependent on said plaintext in place of said plurality of random numbers.

29. (Currently Amended) A decrypting method comprising:

(a) determining whether a decrypting operation at a current decrypting stage should be changed, based on decrypting stage data at a previous decrypting stage, said decrypting stage data at said previous decrypting stage indicating an decrypting state at each of said plurality of processing stages;

(b) changing said decrypting operation at said current decrypting stage when it is determined that said decrypting operation at said next decrypting stage should be changed;

(c) carrying out said decrypting operation at said current decrypting stage a plurality of times to a ciphertext using intermediate data at said current decrypting stage; and

(d) executing said steps (a) to (c) to each of a plurality of decrypting stages to produce a plaintext,

wherein said step (b) determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed depending on at least a plurality of random numbers, based on said decrypting stage data at said current decrypting stage from said step (c),

wherein said decrypting stage data includes said intermediate data for said next decrypting stage, and

wherein, in said step (c), said intermediate data at said next decrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said decrypting operation.

wherein said decrypting operation is carried out by:

i) dividing each n-bit word of the plaintext into an upper n bits and a lower n bits, n being an even integer value greater than or equal to 16,

ii) calculating a logical product of the upper n bits of the plaintext with at least one of said plurality of random numbers to obtain a first result, and

iii) calculating a logical product of the lower n bits of the plaintext with at least one of said plurality of random numbers to obtain a second result,

wherein, in obtaining the first result and the second result, a first subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a first of said plurality of random numbers, a second subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a second of said plurality of random numbers, and a third subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with both the first and second random numbers.

30. (Previously Presented) A decrypting method according to claim 29, wherein said determining includes:

determining whether said intermediate data at said current decrypting stage of said decrypting operation should be changed depending on a plurality of random numbers, based on said decrypting stage data at said previous decrypting stage.

31. (Previously Presented) A decrypting method according to-claim 30, wherein said changing includes:

changing said intermediate data at said current decrypting stage depending on said ciphertext or a data dependent on said ciphertext in place of said plurality of random numbers.

32. (Previously Presented) A decrypting method according to claim 29, wherein said determining includes:

determining whether a decrypting procedure at said current decrypting stage of said decrypting operation should be changed depending on a plurality of random numbers, based on said decrypting stage data at said previous decrypting stage, and

wherein said changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said plurality of random numbers.

33. (Previously Presented) A decrypting method according to claim 32, wherein said changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said ciphertext or a data dependent on said ciphertext in place of said plurality of random numbers.

34. (Previously Presented) A decrypting method according to claim 29, wherein said determining includes:

determining whether said decrypting operation at said current decrypting stage should be changed depending on a plurality of random numbers, based on said decrypting stage data at said previous decrypting stage, and

wherein said changing includes:

inserting a delay time in said decrypting operation at said current decrypting stage depending on said plurality of random numbers.

35. (Previously Presented) A decrypting method according to claim 34, wherein said changing includes:

inserting said delay time in said decrypting operation at said current decrypting stage depending on said ciphertext or a data dependent on said ciphertext in place of said plurality of random numbers.

36. (Currently Amended) An encrypting and decrypting method comprising:

(a) determining whether an inputted instruction is an encrypt instruction or a decrypt instruction;

(b) determining whether said encrypting operation to a text at a current encrypting stage of an encrypting operation should be changed, based on said encrypting stage data at a previous encrypting stage, said encrypting stage data at said current encrypting stage indicating an encrypting state at said current encrypting stage;

(c) changing said encrypting operation to said text at said current encrypting stage when it is determined that said encrypting operation to said text at said current encrypting stage should be changed;

(d) carrying out said encrypting operation to said text using first intermediate data at current encrypting stage of said encrypting operation;

(e) executing said steps (b) to (d) for each of a plurality of encrypting stages of said encrypting operation to said text in response to said encrypt instruction to produce a ciphertext;

(f) determining whether said decrypting operation to said text at a current decrypting stage should be changed, based on said decrypting stage data at a previous decrypting stage, said decrypting stage data at said current decrypting stage indicating an decrypting state at said current decrypting stage;

(g) changing said decrypting operation to said text at said current decrypting stage when it is determined that said decrypting operation to said text at said current decrypting stage should be changed;

(h) carrying out said decrypting operation to said text using second intermediate data at said current decrypting stage; and

(i) executing said steps (f) to (h) for each of a plurality of decrypting stages of said encrypting operation to said text in response to said decrypt instruction to produce a plaintext,

wherein said step (b) determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting stage data at said current encrypting stage from said step (c),

wherein said encrypting stage data includes said intermediate data at said next encrypting stage,

wherein, in said step (c), said intermediate data at said next encrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation,

wherein said step (f) determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed depending on at least a plurality of

random numbers, based on said decrypting stage data at said current decrypting stage from said step (h),

wherein said decrypting stage data includes said intermediate data for said next decrypting stage, and

wherein, in said step (f), said intermediate data at said next decrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said decrypting operation,

wherein said encrypting operation is carried out by:

i) dividing each n-bit word of the plaintext into an upper n bits and a lower n bits, n being an even integer value greater than or equal to 16,

ii) calculating a logical product of the upper n bits of the plaintext with at least one of said plurality of random numbers to obtain a first result, and

iii) calculating a logical product of the lower n bits of the plaintext with at least one of said plurality of random numbers to obtain a second result,

wherein, in obtaining the first result and the second result, a first subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a first of said plurality of random numbers, a second subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a second of said plurality of random numbers, and a third subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with both the first and second random numbers.

37. (Previously Presented) An encrypting and decrypting method according to claim 36, wherein said (b) determining includes:

determining whether said first intermediate data at said current encrypting stage of said encrypting operation should be changed depending on a first plurality of random numbers, based on said encrypting stage data at said previous encrypting stage,

wherein said (f) determining includes:

determining whether said second intermediate data at said current decrypting stage of said decrypting operation should be changed depending on a second plurality of random numbers, based on said decrypting stage data at said previous decrypting stage.

38. (Previously Presented) An encrypting and decrypting method according to claim 37, wherein said (c) changing includes:

changing said first intermediate data at said current encrypting stage depending on said text or a data dependent on said text in place of said first plurality of random numbers, and

wherein said (g) changing includes:

changing said second intermediate data at said current decrypting stage depending on said text or said data dependent on said text in place of said second plurality of random numbers.

39. (Previously Presented) An encrypting and decrypting method according to claim 36, wherein said (b) determining includes:

determining whether an encrypting procedure at said current encrypting stage of said encrypting operation should be changed depending on a first plurality of random numbers, based on said encrypting stage data at said previous encrypting stage,

wherein said (f) determining includes:

determining whether a decrypting procedure at said current decrypting stage of said decrypting operation should be changed depending on a second plurality of random numbers, based on said decrypting stage data at said previous decrypting stage,

wherein said (c) changing includes:

changing said encrypting procedure at said current encrypting stage of said encrypting operation depending on said first plurality of random numbers, and

wherein said (g) changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said second plurality of random numbers.

40. (Previously Presented) An encrypting and decrypting method according to claim 39, wherein said (c) changing includes:

changing said encrypting procedure at said current encrypting stage of said encrypting operation depending on said text or a data dependent on said text in place of said first plurality of random numbers, and

wherein said (g) changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said text or said data dependent on said text in place of said second plurality of random numbers.

41. (Previously Presented) An encrypting and decrypting method according to claim 36, wherein said (b) determining includes:

determining whether said encrypting operation at said current encrypting stage should be changed depending on a first plurality of random numbers, based on said encrypting stage data at said previous encrypting stage,

wherein said (f) determining includes:

determining whether said decrypting operation at said current decrypting stage should be changed depending on a second plurality of random numbers, based on said decrypting stage data at said previous decrypting stage,

wherein said (c) changing includes:

inserting a first delay time in said encrypting operation at said current encrypting stage depending on said first plurality of random numbers, and wherein said (g) changing includes:

inserting a second delay time in said decrypting operation at said current decrypting stage depending on said second plurality of random numbers.

42. (Previously Presented) An encrypting and decrypting method according to claim 41, wherein said (c) changing includes:

inserting said first delay time in said encrypting operation at said current encrypting stage depending on said text or a data dependent on said text in place of said first plurality of random numbers,

wherein said (f) changing includes:

inserting said second delay time in said decrypting operation at said current decrypting stage depending on said text or said data dependent on said text in place of said second plurality of random numbers.

43. (Currently Amended) A recording medium which stores a problem for an encrypting method, wherein said encrypting method comprises:

(a) determining whether an encrypting operation at a current encrypting stage should be changed, based on encrypting stage data at a previous encrypting stage, said encrypting stage data at said previous encrypting stage indicating an encrypting state at said previous encrypting stage;

(b) changing said encrypting operation at said current encrypting stage when it is determined that said encrypting operation at said current encrypting stage should be changed;

(c) carrying out said encrypting operation at said current encrypting stage a plurality of times to a plaintext using intermediate data at said current encrypting stage; and

(d) executing said steps (a) to (c) to each of a plurality of said encrypting stages of said encrypting operation to produce a ciphertext,

wherein said step (b) determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting stage data at said current encrypting stage from said step (c),

wherein said encrypting stage data includes said intermediate data at said next encrypting stage, and

wherein, in said step (c), said intermediate data at said next encrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation,

wherein said encrypting operation is carried out by:

i) dividing each n-bit word of the plaintext into an upper n bits and a lower n bits, n being an even integer value greater than or equal to 16,

ii) calculating a logical product of the upper n bits of the plaintext with at least one of said plurality of random numbers to obtain a first result, and

iii) calculating a logical product of the lower n bits of the plaintext with at least one of said plurality of random numbers to obtain a second result,

wherein, in obtaining the first result and the second result, a first subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a first of said plurality of random numbers, a second subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a second of said plurality of random numbers, and a third subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with both the first and second random numbers.

44. (Previously Presented) A recording medium according to claim 43, wherein said determining includes:

determining whether said intermediate data at said current encrypting stage of said encrypting operation should be changed depending on a plurality of random numbers, based on said encrypting-stage data at said previous encrypting stage.

45. (Previously Presented) A recording medium according to claim 44, wherein said changing includes:

changing said intermediate data at said current encrypting stage depending on said plaintext or a data dependent on said plaintext in place of said plurality of random numbers.

46. (Previously Presented) A recording medium according to claim 43, wherein said determining includes:

determining whether an encrypting procedure at said current encrypting stage of said encrypting operation should be changed depending on a plurality of random numbers, based on said encrypting stage data at said previous encrypting stage, and

wherein said changing includes:

changing said encrypting procedure at said current encrypting stage of said encrypting operation depending on said plurality of random numbers.

47. (Previously Presented) A recording medium according to claim 46, wherein said changing includes:

changes said encrypting procedure at said next encrypting stage of said encrypting operation depending on said plaintext or a data dependent on said plaintext in place of said plurality of random numbers.

48. (Previously Presented) A recording medium according to claim 43, wherein said determining includes:

determining whether said encrypting operation at said current encrypting stage should be changed depending on a plurality of random numbers, based on said encrypting stage data at said previous encrypting stage, and

wherein said changing includes:

inserting a delay time in said encrypting operation at said current encrypting stage depending on said plurality of random numbers.

49. (Currently Amended) A recording medium according to claim 48, wherein said changing includes:

inserting said delay time in said encrypting operation at said current encrypting stage depending on said plaintext or a data dependent on said plaintext in place of said plurality of random numbers.

50. (Currently Amended) A recording medium which stores a program for a decrypting method, wherein said decrypting method comprises:

(a) determining whether a decrypting operation at a current decrypting stage should be changed, based on decrypting stage data at a previous decrypting stage, said decrypting stage data at said previous decrypting stage indicating an decrypting state at each of said plurality of processing stages;

(b) changing said decrypting operation at said current decrypting stage when it is determined that said decrypting operation at said next decrypting stage should be changed;

(c) carrying out said decrypting operation at said current decrypting stage a plurality of times to a ciphertext using intermediate data at said current decrypting stage; and

(d) executing said steps (a) to (c) to each of a plurality of decrypting stages to produce a plaintext,

wherein said step (b) determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed depending on at least a plurality of random numbers, based on said decrypting stage data at said current decrypting stage from said step (c),

wherein said decrypting stage data includes said intermediate data for said next decrypting stage, and

wherein, in said step (c), said intermediate data at said next decrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said decrypting operation,

wherein said decrypting operation is carried out by:

i) dividing each n-bit word of the plaintext into an upper n bits and a lower n bits, n being an even integer value greater than or equal to 16,

ii) calculating a logical product of the upper n bits of the plaintext with at least one of said plurality of random numbers to obtain a first result, and

iii) calculating a logical product of the lower n bits of the plaintext with at least one of said plurality of random numbers to obtain a second result,

wherein, in obtaining the first result and the second result, a first subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a first of said plurality of random numbers, a second subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a second of said plurality of random numbers, and a third subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with both the first and second random numbers.

51. (Previously Presented) A recording medium according to claim 50, wherein said determining includes:

determining whether said intermediate data at said current decrypting stage of said decrypting operation should be changed depending on a plurality of random numbers, based on said decrypting stage data at said previous decrypting stage.

52. (Previously Presented) A recording medium according to claim 51, wherein said changing includes:

changing said intermediate data at said current decrypting stage depending on said ciphertext or a data dependent on said ciphertext in place of said plurality of random numbers.

53. (Previously Presented) A recording medium according to claim 50, wherein said determining includes:

determining whether a decrypting procedure at said current decrypting stage of said decrypting operation should be changed depending on a plurality of random numbers, based on said decrypting stage data at said previous decrypting stage, and

wherein said changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said plurality of random numbers.

54. (Previously Presented) A recording medium according to claim 53, wherein said changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said ciphertext or a data dependent on said ciphertext in place of said plurality of random numbers.

55. (Previously Presented) A recording medium according to claim 50, wherein said determining includes:

determining whether said decrypting operation at said current decrypting stage should be changed depending on a plurality of random numbers, based on said decrypting stage data at said previous decrypting stage, and

wherein said changing includes:

inserting a delay time in said decrypting operation at said current decrypting stage depending on said plurality of random numbers.

56. (Previously Presented) A recording medium according to claim 55, wherein said changing includes:

inserting said delay time in said decrypting operation at said current decrypting stage depending on said ciphertext or a data dependent on said ciphertext in place of said plurality of random numbers.

57. (Currently Amended) A recording medium which stores a problem for an encrypting and decrypting method, wherein said encrypting and decrypting method comprises:

(a) determining whether an inputted instruction is an encrypt instruction or a decrypt instruction;

(b) determining whether said encrypting operation to a text at a current encrypting stage of an encrypting operation should be changed, based on said encrypting stage data at a previous encrypting stage, said encrypting stage data at said current encrypting stage indicating an encrypting state at said current encrypting stage;

(c) changing said encrypting operation to said text at said current encrypting stage when it is determined that said encrypting operation to said text at said current encrypting stage should be changed;

(d) carrying out said encrypting operation to said text using first intermediate data at current encrypting stage of said encrypting operation;

(e) executing said steps (b) to (d) for each of a plurality of encrypting stages of said encrypting operation to said text in response to said encrypt instruction to produce a ciphertext;

(f) determining whether said decrypting operation to said text at a current decrypting stage should be changed, based on said decrypting stage data at a previous decrypting stage, said decrypting stage data at said current decrypting stage indicating an decrypting state at said current decrypting stage;

(g) changing said decrypting operation to said text at said current decrypting stage when it is determined that said decrypting operation to said text at said current decrypting stage should be changed;

(h) carrying out said decrypting operation to said text using second intermediate data at said current decrypting stage; and

(i) executing said steps (f) to (h) for each of a plurality of decrypting stages of said encrypting operation to said text in response to said decrypt instruction to produce a plaintext,

wherein said step (b) determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting stage data at said current encrypting stage from said step (c),

wherein said encrypting stage data includes said intermediate data at said next encrypting stage,

wherein, in said step (c), said intermediate data at said next encrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation,

wherein said step (f) determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed depending on at least a plurality of random numbers, based on said decrypting stage data at said current decrypting stage from said step (h),

wherein said decrypting stage data includes said intermediate data for said next decrypting stage, and

wherein, in said step (f), said intermediate data at said next decrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said decrypting operation,

wherein said encrypting operation is carried out by:

i) dividing each n-bit word of the plaintext into an upper n bits and a lower n bits, n being an even integer value greater than or equal to 16,

ii) calculating a logical product of the upper n bits of the plaintext with at least one of said plurality of random numbers to obtain a first result, and

iii) calculating a logical product of the lower n bits of the plaintext with at least one of said plurality of random numbers to obtain a second result,

wherein, in obtaining the first result and the second result, a first subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a first of said plurality of random numbers, a second subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a second of said plurality of random numbers, and a third subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with both the first and second random numbers.

58. (Previously Presented) A recording medium according to claim 57, wherein said (b) determining includes:

determining whether said first intermediate data at said current encrypting stage of said encrypting operation should be changed depending on a first plurality of random numbers, based on said encrypting stage data at said previous encrypting stage,

wherein said (f) determining includes:

determining whether said second intermediate data at said current decrypting stage of said decrypting operation should be changed depending on a second plurality of random numbers, based on said decrypting stage data at said previous decrypting stage,

wherein said encrypting stage data includes said first intermediate data at said current encrypting stage and said decrypting stage data includes said second intermediate data for said current decrypting stage,

wherein said (c) changing includes:

changing said first intermediate data at said current encrypting stage depending on said first plurality of random numbers, and

wherein said (g) changing includes:

changing said second intermediate data at said current decrypting stage depending on said second plurality of random numbers.

59. (Previously Presented) A recording medium according to claim 58, wherein said (c) changing includes:

changing said first intermediate data at said current encrypting stage depending on said text or a data dependent on said text in place of said first plurality of random numbers, and

wherein said (g) changing includes:

changing said second intermediate data at said current decrypting stage depending on said text or said data dependent on said text in place of said second plurality of random numbers.

60. (Previously Presented) A recording medium according to claim 57, wherein said (b) determining includes:

determining whether an encrypting procedure at said current encrypting stage of said encrypting operation should be changed depending on a first plurality of random numbers, based on said encrypting stage data at said previous encrypting stage,

wherein said (f) determining includes:

determining whether a decrypting procedure at said current decrypting stage of said decrypting operation should be changed depending on a second plurality of random numbers, based on said decrypting stage data at said previous decrypting stage, wherein said (c) changing includes:

changing said encrypting procedure at said current encrypting stage of said encrypting operation depending on said first plurality of random numbers, and

wherein said (g) changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said second plurality of random numbers.

61. (Previously Presented) A recording medium according to claim 60, wherein said (c) changing includes:

changing said encrypting procedure at said current encrypting stage of said encrypting operation depending on said text or a data dependent on said text in place of said first plurality of random numbers, and

wherein said (g) changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said text or said data dependent on said text in place of said second plurality of random numbers.

62. (Previously Presented) A recording medium according to claim 57, wherein said (b) determining includes:

determining whether said encrypting operation at said current encrypting stage should be changed depending on a first plurality of random numbers, based on said encrypting stage data at said previous encrypting stage,

wherein said (f) determining includes:

determining whether said decrypting operation at said current decrypting stage should be changed depending on a second plurality of random numbers, based on said decrypting stage data at said previous decrypting stage,

wherein said (c) changing includes:

inserting a first delay time in said encrypting operation at said current encrypting stage depending on said first plurality of random numbers, and

wherein said (g) changing includes:

inserting a second delay time in said decrypting operation at said current decrypting stage depending on said second plurality of random numbers.

63. (Previously Presented) A recording medium according to claim 62, wherein said (c) changing includes:

inserting said first delay time in said encrypting operation at said current encrypting stage depending on said text or a data dependent on said text in place of said first plurality of random numbers,

wherein said (f) changing includes:

inserting said second delay time in said decrypting operation at said current decrypting stage depending on said text or said data dependent on said text in place of said second plurality of random numbers.